TNGNET B.V.
Zuidewijnlaan 14
4706 VL Roosendaal
The Netherlands

Company information
VAT: NL855609928B01
CoC: 64310051
Phone: +31 20 210 6040

TNGNET
The Next Generation Network
WWW.TNGNET.COM

Technical and Organizational Measures (TOMs) – TNGNET B.V.

TNGNET B.V. implements organizational and technical safeguards designed to ensure the confidentiality, integrity, and availability of personal data in accordance with Article 32 of the General Data Protection Regulation (GDPR). These measures apply to all infrastructure, systems, and services operated by TNGNET, including its additional brand names, within data centers located in the Netherlands.

1. Purpose and Scope

This document provides an overview of TNGNET's technical and organizational measures for the protection of customer and personal data. The controls outlined below are applied across all TNGNET environments and form part of TNGNET's continuous compliance framework.

2. Physical Security

TNGNET's infrastructure is hosted exclusively in the Netherlands within ISO 27001-certified data centers. TNGNET occupies fully dedicated racks under its sole control. These racks are individually locked, and only authorized TNGNET personnel have physical access. Data center facilities include 24/7 staffed security, CCTV surveillance, biometric or access-card entry systems, visitor registration, and environmental controls such as fire suppression and redundant power feeds.

3. Logical Access Controls

Access to management systems and customer infrastructure is strictly limited to authorized TNGNET staff. Multi-factor authentication (MFA), key-based authentication, and IP whitelisting are used for administrative access. Access rights are reviewed regularly and immediately revoked upon role changes or termination.

4. Data Encryption and Protection

All administrative and service connections use secure encrypted channels (TLS, SSH). Customer data transmitted over public networks is encrypted in transit. Sensitive internal data may also be encrypted at rest. Encryption keys are managed securely with periodic rotation and strict access control. Credentials and passwords are hashed using strong cryptographic algorithms and never stored in plaintext.

5. Network and Communication Security

TNGNET maintains logical and physical separation between network segments to prevent unauthorized access. Firewalls and intrusion prevention systems are deployed at all perimeter and management layers. DDoS mitigation, using NBIP NaWaS protection and Liberty Global's DDoS mitigation and scrubbing services. Continuous monitoring is performed to detect and respond to anomalous traffic and potential threats.

TNGNET operates its own dark fiber network interconnected with major Tier 1 carriers and peering exchanges. These interconnections enhance capacity, redundancy, performance, and overall network resilience and security.

6. Operational Security

TNGNET follows secure operational practices including routine system patching, vulnerability management, and access log reviews. Backups are performed regularly and tested for integrity. All changes to production systems follow a documented change management process requiring approval and testing prior to deployment.

7. Incident and Breach Management

TNGNET maintains procedures for identifying, reporting, and responding to security incidents. Any personal data breach is promptly evaluated, with affected customers notified within 48 hours when required. Root cause analysis and corrective actions are documented for continuous improvement.

8. Business Continuity and Disaster Recovery

TNGNET operates redundant infrastructure components for power, cooling, networking, and storage within the EU. Backup and disaster recovery processes are tested annually. Key systems are designed for high availability and rapid recovery in the event of hardware or service failures.

9. Organizational Measures

All TNGNET employees sign confidentiality agreements and receive regular security and GDPR awareness training. Access to systems containing personal data is restricted to personnel with a legitimate operational need. TNGNET's internal policies define roles, responsibilities, and disciplinary measures related to data protection and information security.

10. Compliance and Review

TNGNET periodically reviews and updates these Technical and Organizational Measures to reflect technological advancements, risk assessments, and legal or regulatory requirements. Controls are designed to align with internationally recognized standards such as ISO 27001 and NEN 7510.